



@jackfarley248
@swiftforensics

Windows Store & Apps (APPX) analysis

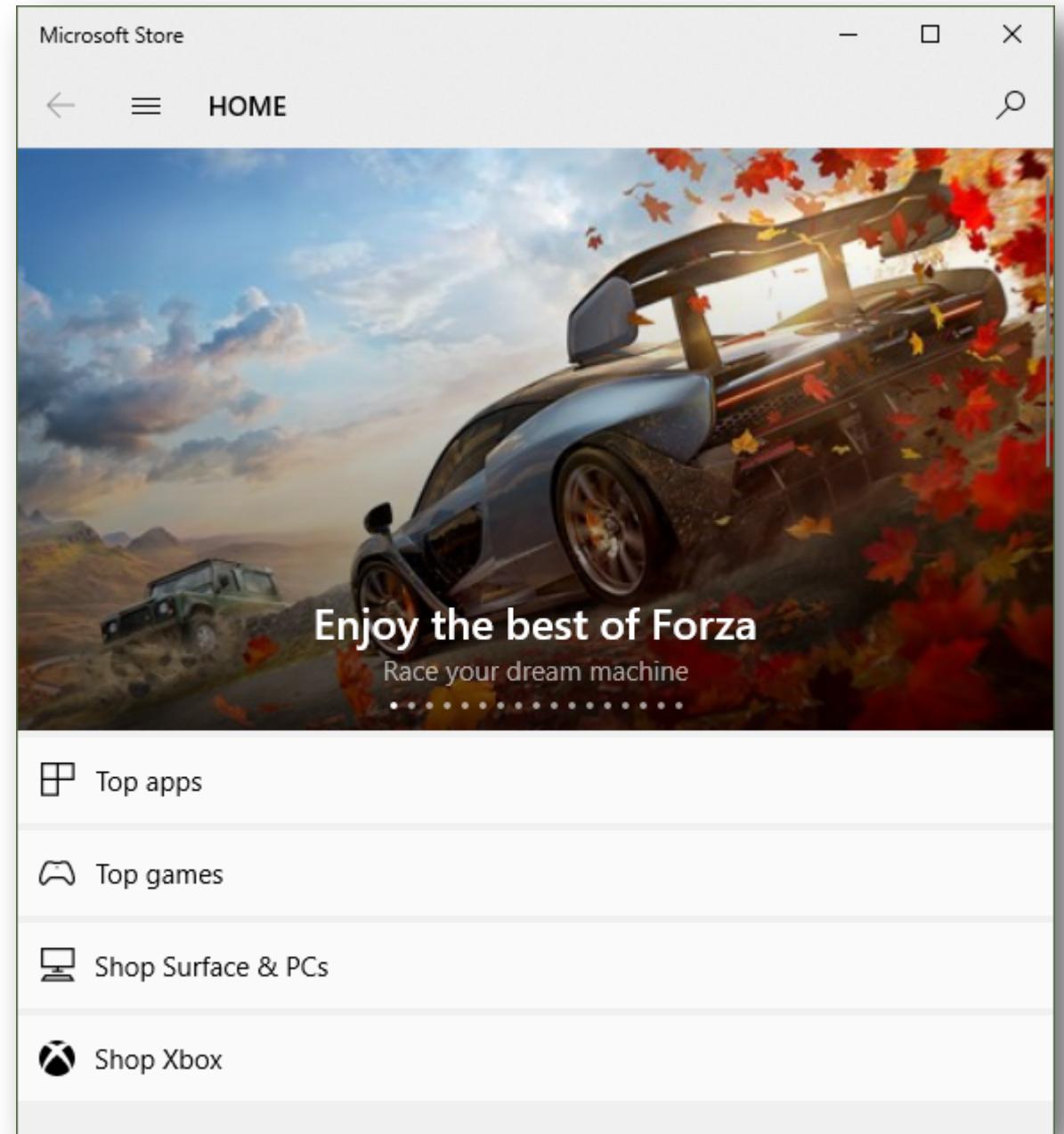
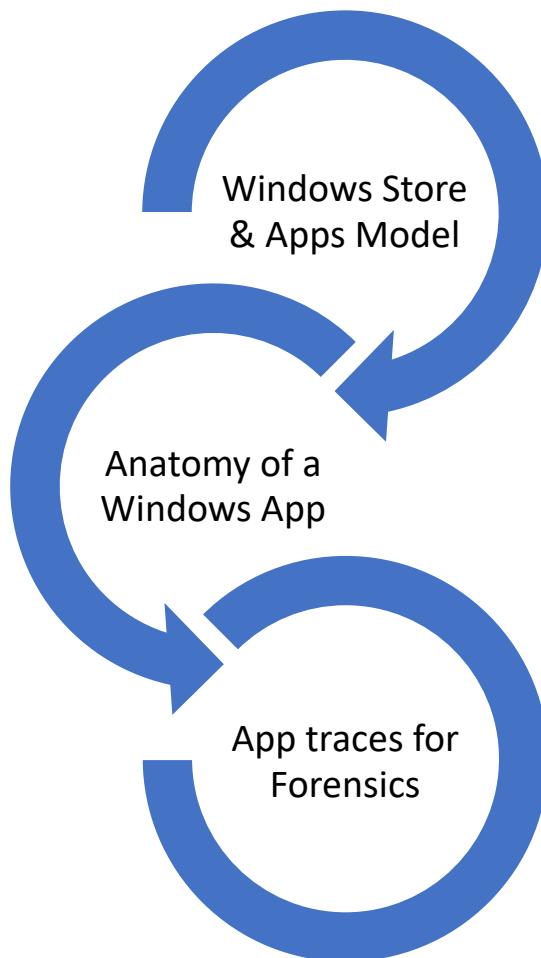
Yogesh Khatri

Jack Farley

Champlain College



Agenda



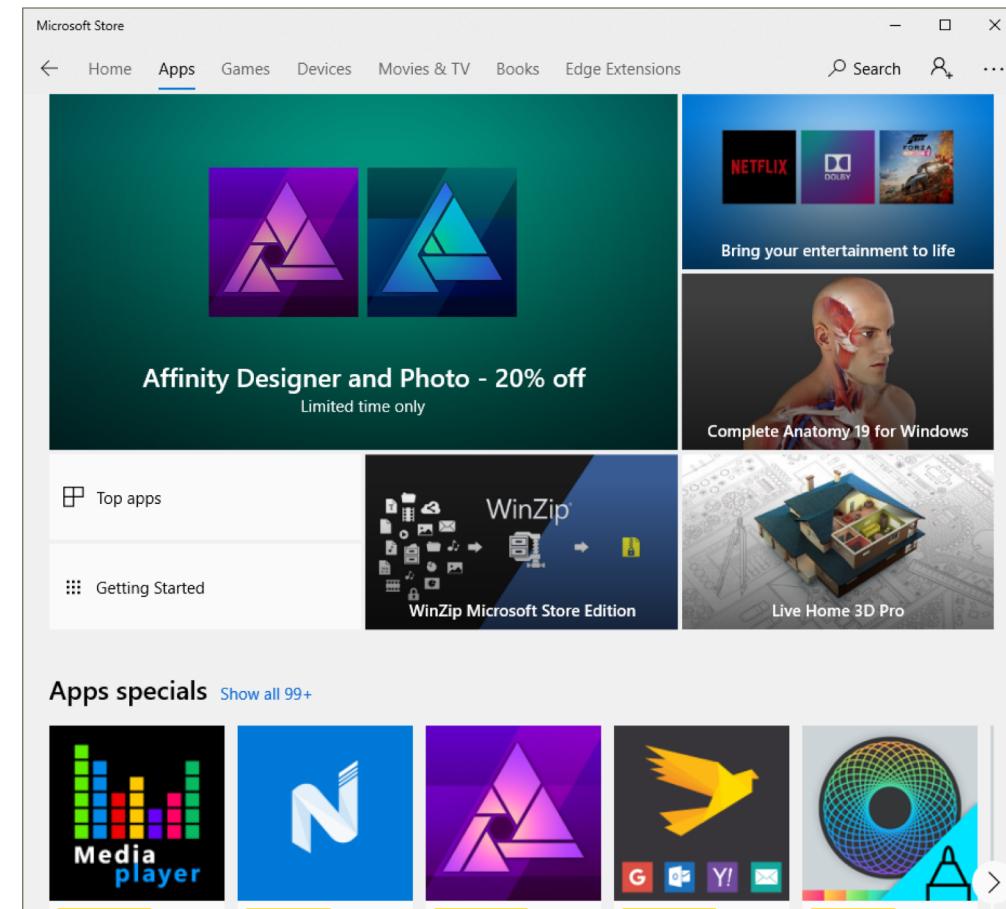
Universal Windows Platform – UWP

UWP apps were earlier called Metro Apps (windows 8), Modern Apps, then Universal Apps (windows 10)



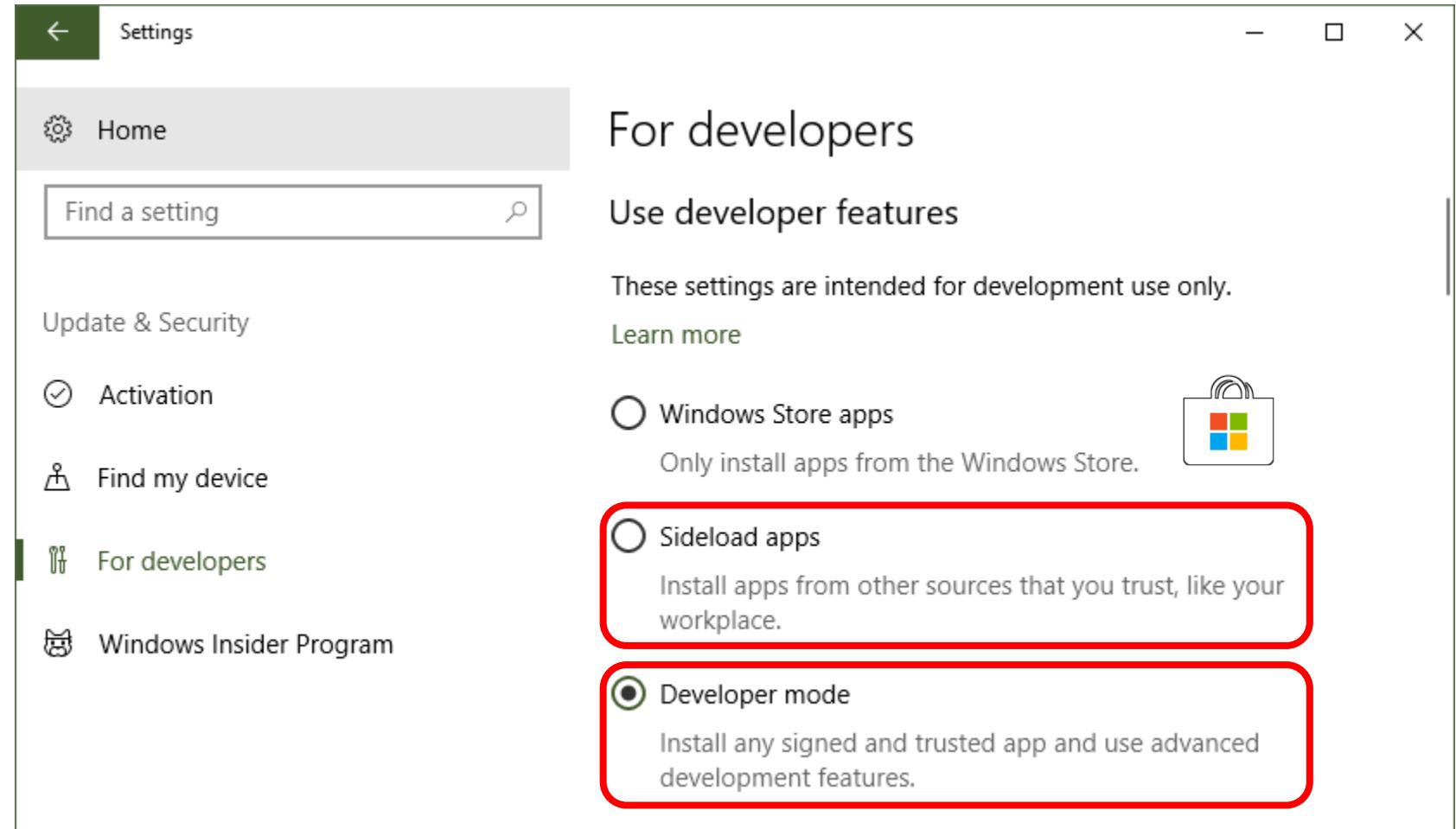
UWP App Model

- Downloads as APPX package
- Secure App delivery (via Microsoft Store)
- Runs in Sandboxed environment
 - No registry access
 - No file system access outside sandbox folder
 - Must use Windows Runtime API (winRT)
 - Very limited win32 API access
 - Apps must declare device resources used (microphone, camera, ..)
- Apps can interact with Windows Timeline, Cortana, Live tiles, send Push Notifications



Installing AppX outside the Store

- Sideload allows trusted apps only!
- Dev mode allows any untrusted app



Getting Appx info on live machines

```
Windows PowerShell
PS C:\Users\khatri> Get-AppxPackage | Where Name -like '*calc*'

Name          : Microsoft.WindowsCalculator
Publisher     : CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Architecture   : X64
ResourceId    :
Version       : 10.1804.2492.0
PackageFullName: Microsoft.WindowsCalculator_10.1804.2492.0_x64__8wekyb3d8bbwe
InstallLocation: C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_10.1804.2492.0_x64__8wekyb3d8bbwe
IsFramework    : False
PackageFamilyName: Microsoft.WindowsCalculator_8wekyb3d8bbwe
PublisherId    : 8wekyb3d8bbwe
IsResourcePackage: False
IsBundle       : False
IsDevelopmentMode: False
Dependencies   : {Microsoft.VCLibs.140.00_14.0.27323.0_x64__8wekyb3d8bbwe,
                  Microsoft.WindowsCalculator_10.1804.2492.0_neutral_split.scale-100_8wekyb3d8bbwe}
IsPartiallyStaged: False
SignatureKind  : Store
Status         : Ok
```

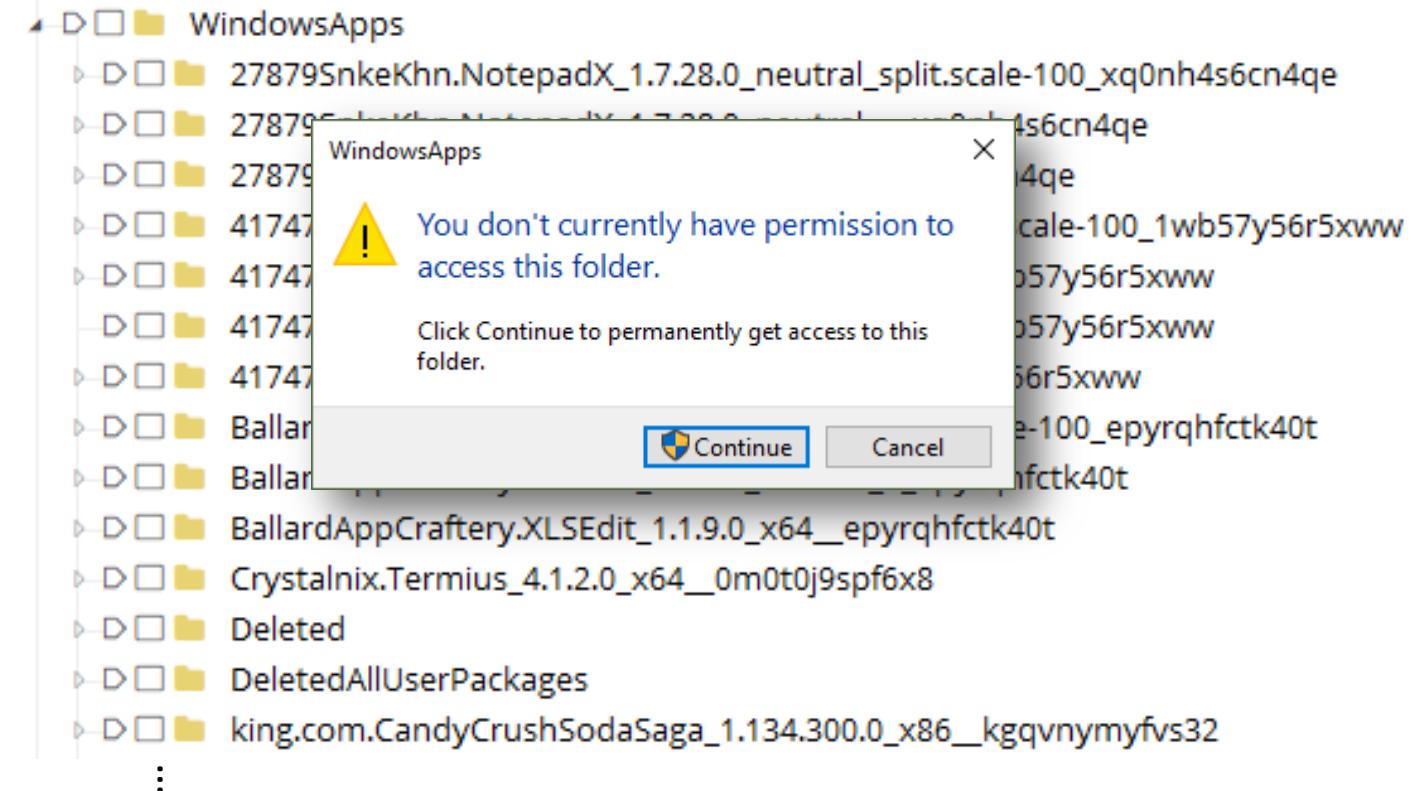
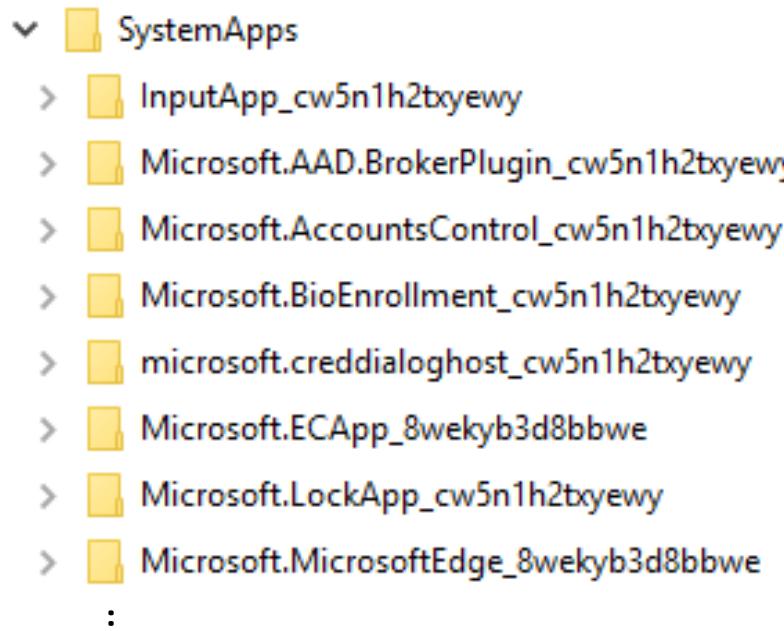
Application Identity

Item	Value
Publisher Name	CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Publisher ID	8wekyb3d8bbwe
Architecture	X64
Version	10.1804.2492.0
Package Name	Microsoft.WindowsCalculator
Package Family Name	Microsoft.WindowsCalculator_8wekyb3d8bbwe
Package Full Name	Microsoft.WindowsCalculator_10.1804.2492.0_x64_8wekyb3d8bbwe
Package-Relative App ID	App
Application User Model ID (AUMID)	Microsoft.WindowsCalculator_8wekyb3d8bbwe!App

App installation Locations

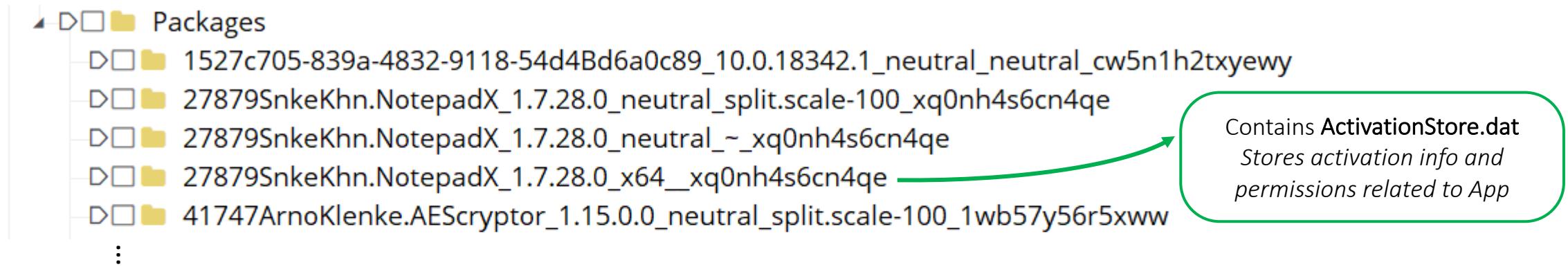
- C:\Windows\SystemApps
- C:\Program Files\WindowsApps

Folder Owned by *TrustedInstaller*
S-1-5-80-956008885-3418522649-
1831038044-1853292631-2271478464



Package Activation Databases & Capability

- C:\ProgramData\Microsoft\Windows\AppRepository\Packages



- Capabilities listed in .xml files in Packages folder

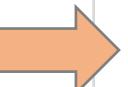
```
<Capabilities>
    <Capability Name="internetClient"/>
    <uap:Capability Name="videosLibrary"/>
    <uap:Capability Name="picturesLibrary"/>
    <DeviceCapability Name="microphone"/>
    <DeviceCapability Name="webcam"/>
    <DeviceCapability Name="location"/>
</Capabilities>
```

Capabilities of Windows 10 Camera App listed in
C:\ProgramData\Microsoft\Windows\AppRepository\Microsoft.WindowsCamera_2019.124.40.0_x64
_8wekyb3d8bbwe.xml

Package licensing info

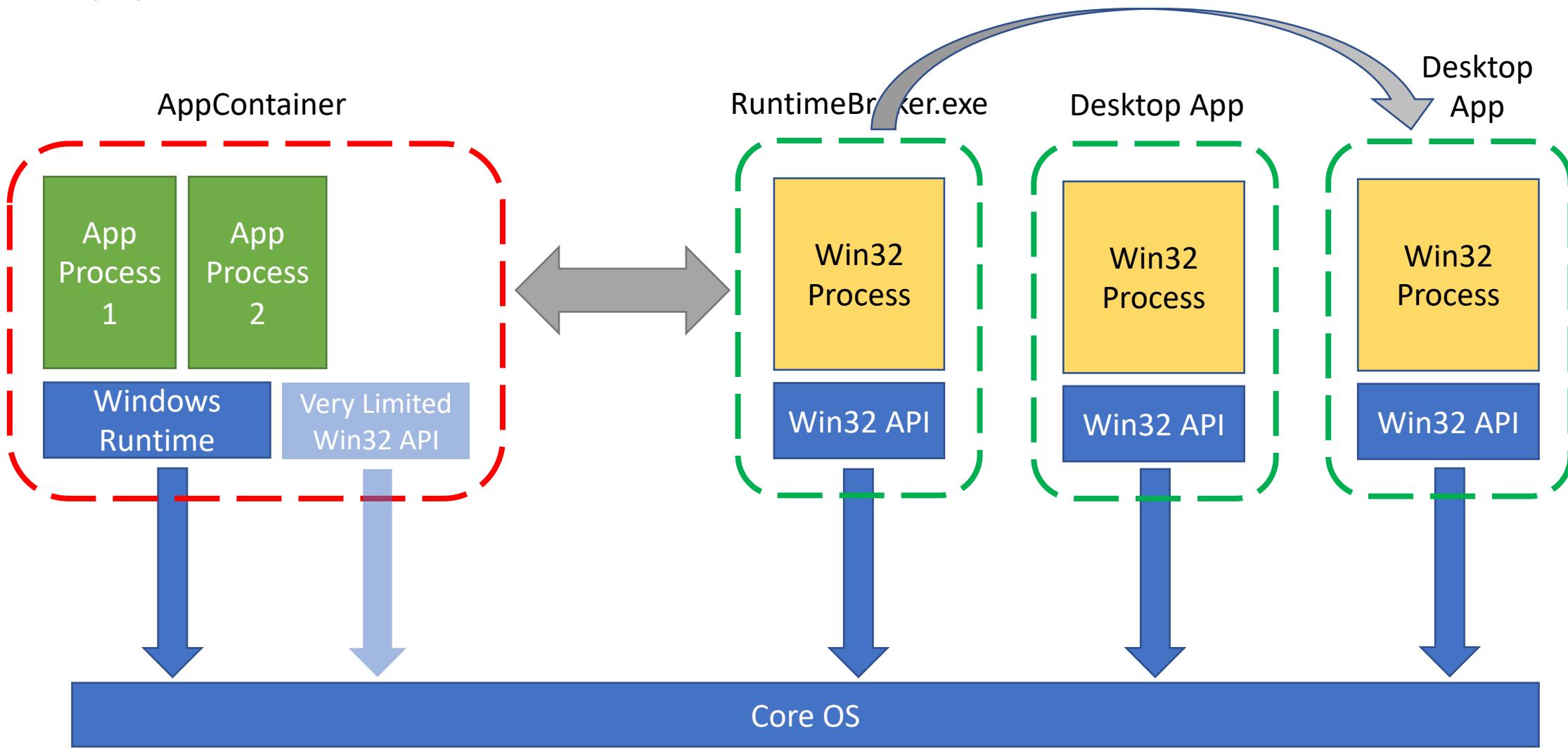
- C:\ProgramData\Microsoft\Windows\ClipSVC\Archive\Apps\

```
bcda97bb-bfd0-2a72-3c90-c8518f3d09ee.xml  
bde1af2b-687b-cd3f-a9b2-148e9eac325c.xml  
c3d42a1a-2f3f-a4a9-6a04-cc1b234485fb.xml  
c94a6c18-d496-da1c-8a02-fc6976e0145e.xml  
ca947da2-7e9a-7249-8095-bceb379c6f74.xml  
cb692946-a9f3-639d-1064-a6d75a01b9c3.xml  
d1ecfce2-f845-c1e9-052b-d2f457c135e6.xml  
d508ba05-d8aa-2836-484d-3833d22fe185.xml  
e2a686b1-b02a-b3e7-90cb-3fa0d708ce04.xml  
e8ac9388-7c9c-19cc-fd4d-cb72bb1544ea.xml  
e8fff2df-6041-8f21-3df7-db31661aa09b.xml
```



```
<License xmlns:xsd="http://www.w3.org/2001/XMLSchema"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:urn:microsoft-com:windows:store:licensing:ls" ID="16245d71-ef86-4482-8454b985c12a8" LicenseID="c94a6c18-d496-da1c-8a02-fc6976e0145e" Version="1.0">
    <Binding Binding_Type="Machine">
        <AssociatedPFNs>Microsoft.WindowsCalculator_8wekyb3d8bbwe</AssociatedPFNs>
        <LeaseRenewalPeriod>129600</LeaseRenewalPeriod>
    </Binding>
    <LicenseInfo Type="Lease" LicenseUsage="Online" LicenseCategory="Machine">
        <IssuedDate>2019-02-23T06:21:27.1947161Z</IssuedDate>
        <LastUpdateDate>2019-02-23T06:21:27.1968828Z</LastUpdateDate>
    </LicenseInfo>
    <CustomPolicies>
        eyJlbmRpdGxlbWVudFNhdGlzZmFjdGlvbiI6Ik9wZW4iLCJpc09mZmxpbmUiOn
    </CustomPolicies>
    <SPLicenseBlock>
        FAAAAALwAAADJAAAAACgAAAAUUAAgBn5nBcAADLAAAAEAAAABhsSsmW1BzaigL8aX
    </SPLicenseBlock>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
```

AppContainer



App processes

Task Manager

File Options View

Processes Performance App history Startup Users Details Services

Name	4% CPU	69% Memory	0% Dis
Apps (18)			
> Google Chrome (31)	0.5%	2,014.6 MB	0.1 M
> Microsoft Excel	0%	24.5 MB	0 M
> Microsoft PowerPoint	0%	13.5 MB	0 M
▼ Photos (2)	0%	144.5 MB	0 M
Photos	0%	129.1 MB	0 M
Runtime Broker	0%	15.4 MB	0 M
> plist Editor Pro (32 bit)	0%	1.1 MB	0 M

< ▲ Fewer details End task

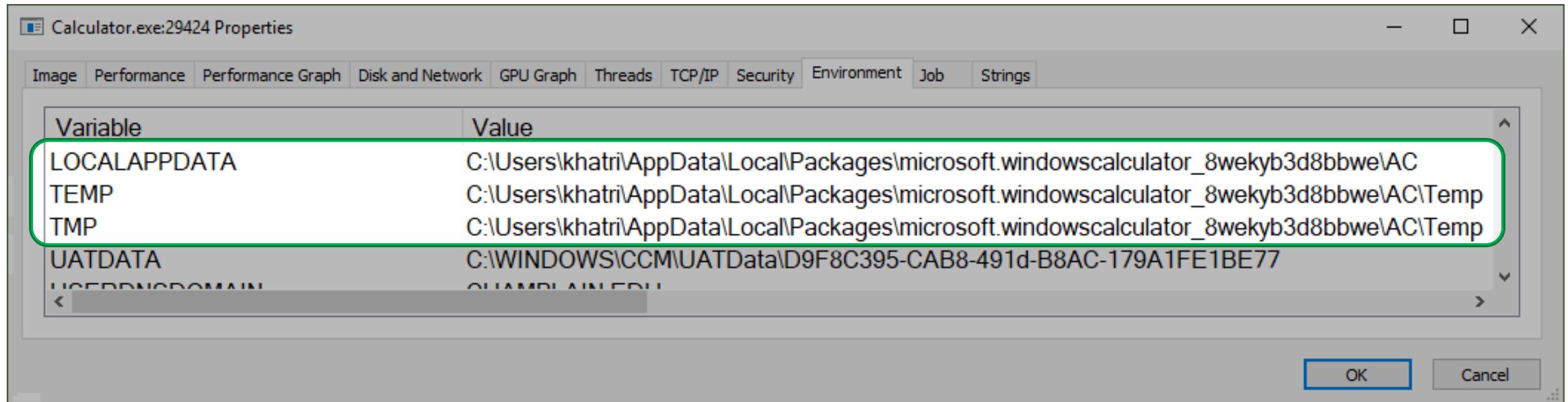
▼ e Microsoft Edge (8)
e Background Tab Pool
e Browser_Broker
e Chakra JIT Compiler
e Microsoft Edge Manager
e Runtime Broker
e Runtime Broker
e User Interface Service
e User Interface Service

Process Details

- Svchost is Parent process for all APPs
- Applications launched cannot be traced back to parent APP

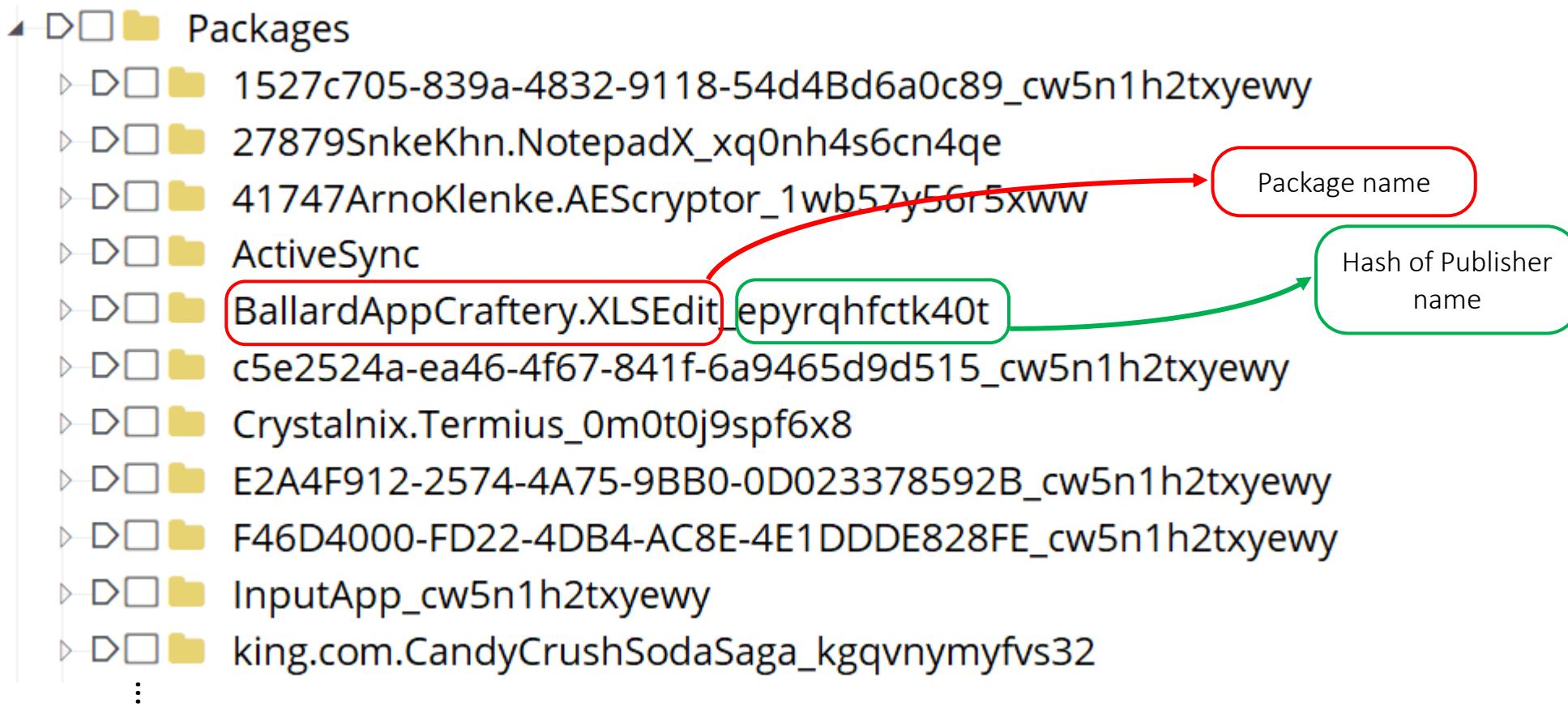
Process	CPU	PID	Description
wininit.exe		900	Windows Start-Up Application
services.exe		972	Services and Controller app
svchost.exe		896	Host Process for Windows Services
svchost.exe		1036	Host Process for Windows Services
WmiPrvSE.exe		5692	WMI Provider Host
ShellExperienceHost.exe	Suspended	8760	Windows Shell Experience Host
RuntimBroker.exe		9016	Runtime Broker
RuntimBroker.exe		9208	Runtime Broker
RuntimBroker.exe		8420	Runtime Broker
EXCEL.EXE	< 0.01	21...	Microsoft Excel
notepad.exe		34...	Notepad
mobsync.exe		9480	Microsoft Sync Center
dllhost.exe		9980	COM Surrogate
WmiPrvSE.exe		13...	WMI Provider Host
dllhost.exe		10...	COM Surrogate
WmiPrvSE.exe		10...	WMI Provider Host
WmiPrvSE.exe		11...	WMI Provider Host
WmiPrvSE.exe		13...	WMI Provider Host
ApplicationFrameHost.exe		4336	Application Frame Host
SystemSettingsBroker.exe		15...	System Settings Broker
dllhost.exe		22...	COM Surrogate
explorer.exe		57...	Windows Explorer
Calculator.exe	Suspended	29...	
RuntimBroker.exe		47...	Runtime Broker
Microsoft.Photos.exe		33...	
SystemSettings.exe		57...	Settings
SystemSettingsAdminFlows.exe		45...	Settings
SearchUI.exe	Suspended	38...	Search and Cortana application
WinStore.App.exe	Suspended	4836	Store
RuntimBroker.exe		45...	Runtime Broker
smartscreen.exe		50...	Windows Defender SmartScreen

Process Environment Variables

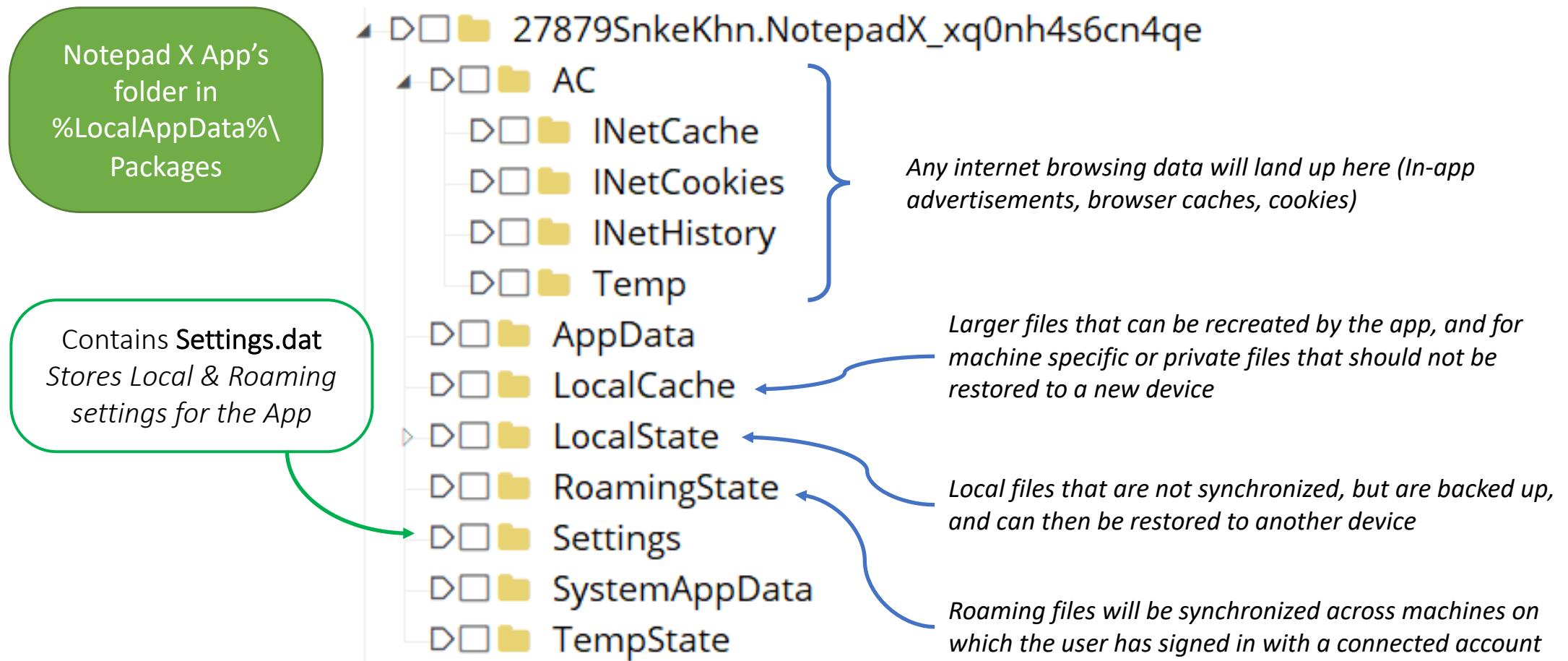


Per user artifacts

- C:\Users\<USER>\AppData\Local\Packages



App Data – Notepad X as example



AppContainer & Capability SIDs

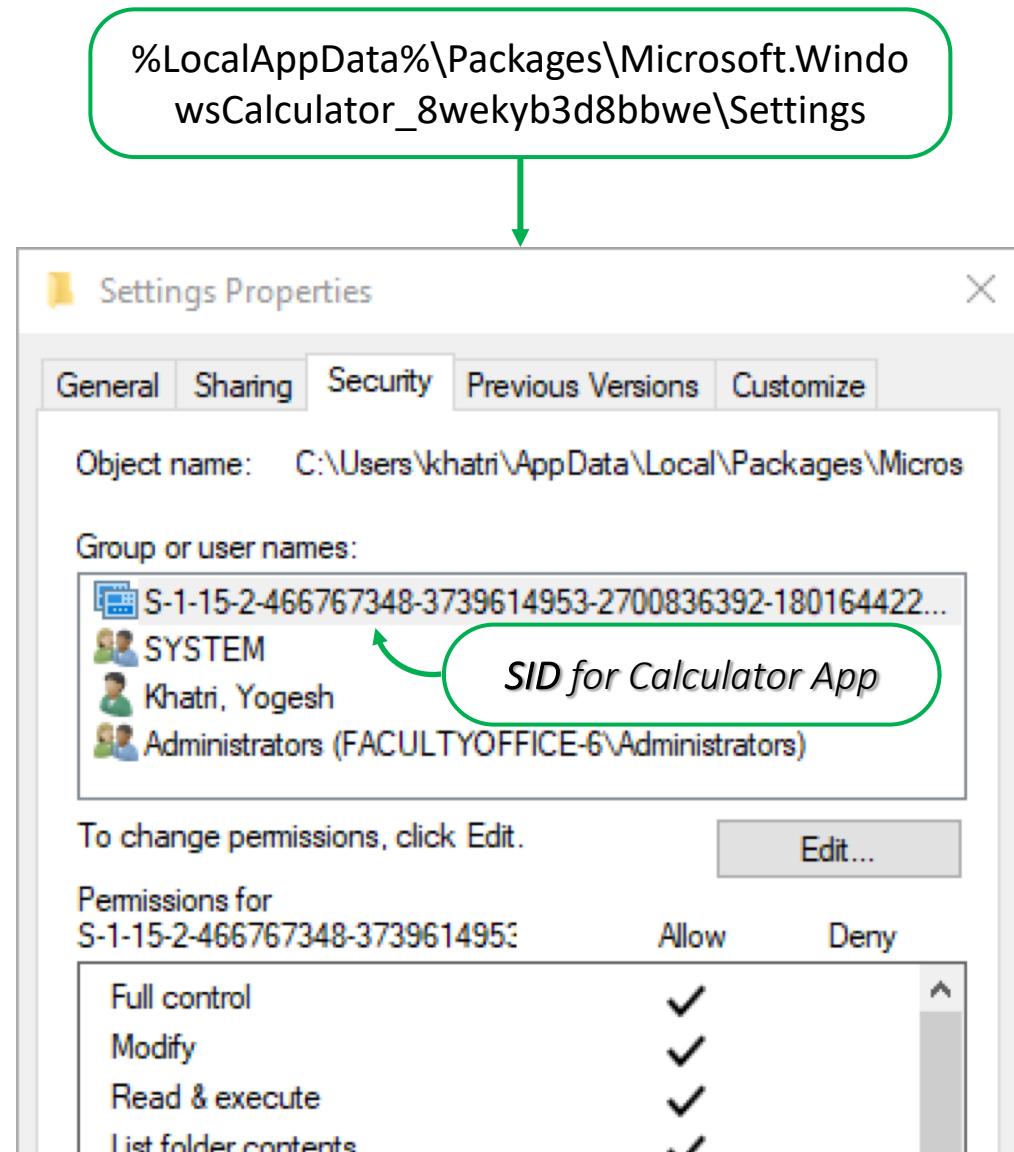
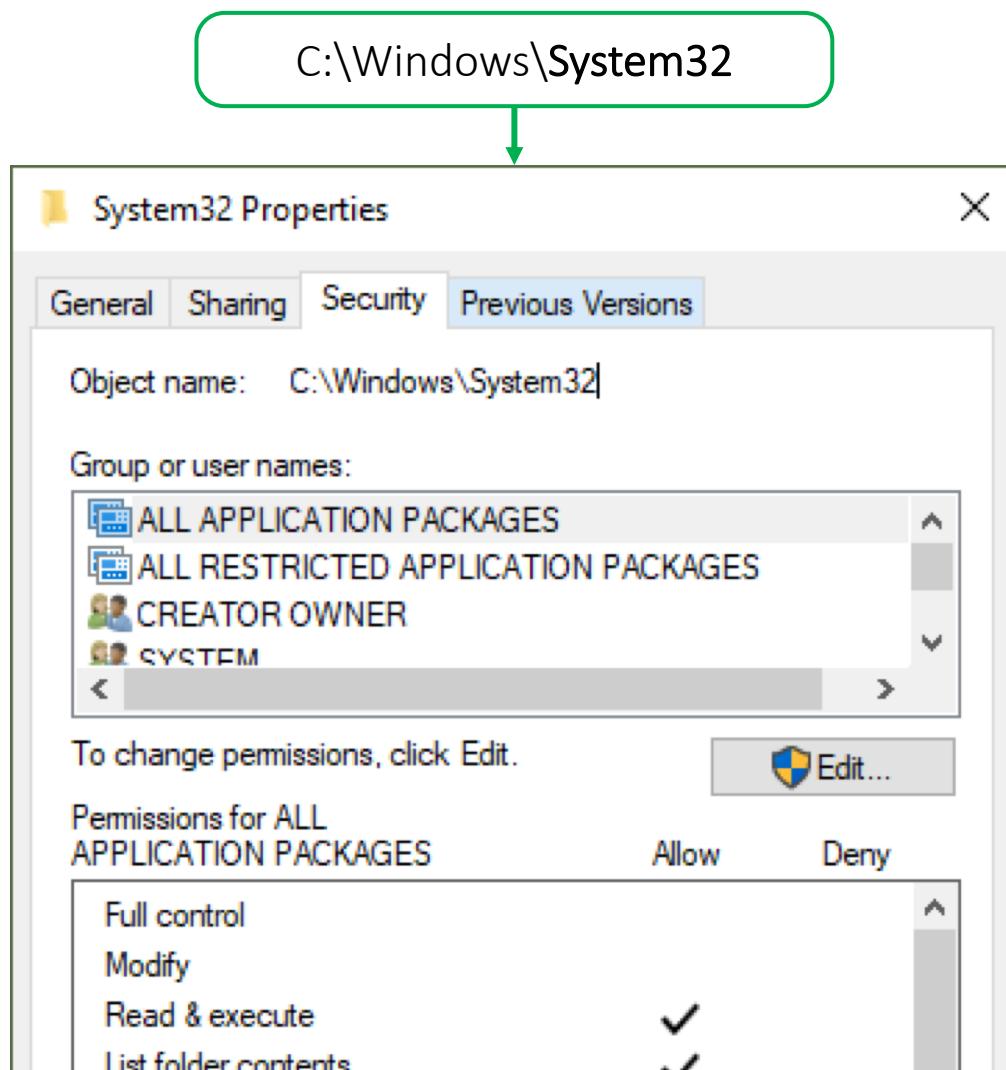
Calculator.exe:29424 Properties

Environment		Job		Strings		
Image	Performance	Performance Graph	Disk and Network	GPU Graph	Threads	TCP/IP
User: CHAMPLAIN\khatri	SID: S-1-5-21-[REDACTED]					
Session: 1	Logon Session: a56bf					
Virtualized: No	Protected: No					

Capabilities

Group	Flags
S-1-15-2-466767348-3739614953-2700836392-1801644223-4227750657-1087833535-2488631167	AppContainer
APPLICATION PACKAGE AUTHORITY\Your Internet connection	Capability
S-1-15-3-1024-2732930991-1716039000-1394599507-3926803129-3068501044-2027633224-866606...	Capability
S-1-15-3-466767348-3739614953-2700836392-1801644223-4227750657-1087833535-2488631167	Capability
BUILTIN\Administrators	Deny
Mandatory Label\Low Mandatory Level	Integrity
CHAMPLAIN\Domain Users	Mandatory
Everyone	Mandatory
BUILTIN\Users	Mandatory
BUILTIN\Performance Log Users	Mandatory
NT AUTHORITY\INTERACTIVE	Mandatory

SID Permissions



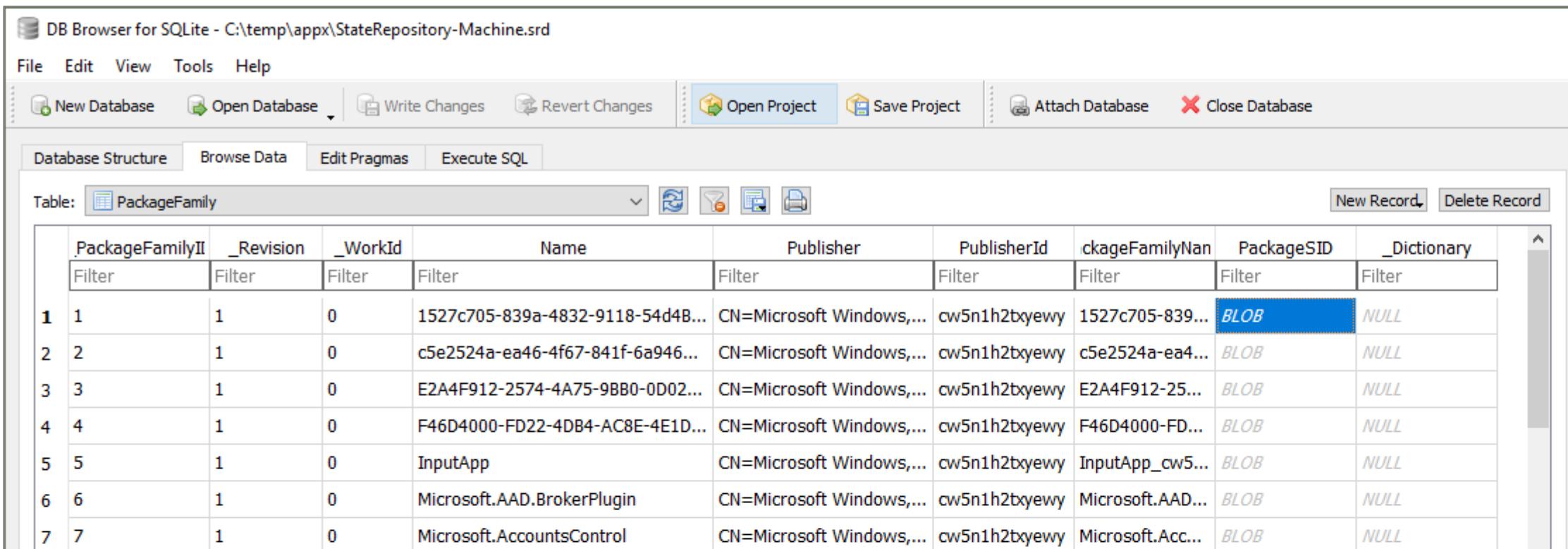
Lets do some Forensics!

- Get information about installed apps
 - Install/Uninstall dates
 - Locations
 - Usage information
 - App settings
 - Execution traces
 - Files/Folders accessed
- Look for uninstalled app remains



Installed App info

- C:\ProgramData\Microsoft\Windows\AppRepository\Packages
 - StateRepository-Machine.srd
 - StateRepository-Deployment.srd



The screenshot shows the DB Browser for SQLite interface with the database file C:\temp\appx\StateRepository-Machine.srd open. The main window displays the 'PackageFamily' table. The table has columns: PackageFamilyID, _Revision, _WorkId, Name, Publisher, PublisherId, PackageFamilyName, PackageSID, and _Dictionary. The data grid contains seven rows of information.

	PackageFamilyID	_Revision	_WorkId	Name	Publisher	PublisherId	PackageFamilyName	PackageSID	_Dictionary
1	1	1	0	1527c705-839a-4832-9118-54d4B...	CN=Microsoft Windows,...	cw5n1h2bxyewy	1527c705-839...	BLOB	NULL
2	2	1	0	c5e2524a-ea46-4f67-841f-6a946...	CN=Microsoft Windows,...	cw5n1h2bxyewy	c5e2524a-ea4...	BLOB	NULL
3	3	1	0	E2A4F912-2574-4A75-9BB0-0D02...	CN=Microsoft Windows,...	cw5n1h2bxyewy	E2A4F912-25...	BLOB	NULL
4	4	1	0	F46D4000-FD22-4DB4-AC8E-4E1D...	CN=Microsoft Windows,...	cw5n1h2bxyewy	F46D4000-FD...	BLOB	NULL
5	5	1	0	InputApp	CN=Microsoft Windows,...	cw5n1h2bxyewy	InputApp_cw5...	BLOB	NULL
6	6	1	0	Microsoft.AAD.BrokerPlugin	CN=Microsoft Windows,...	cw5n1h2bxyewy	Microsoft.AAD...	BLOB	NULL
7	7	1	0	Microsoft.AccountsControl	CN=Microsoft Windows,...	cw5n1h2bxyewy	Microsoft.Acc...	BLOB	NULL

Query to extract App information

```
SELECT DISTINCT * FROM
(SELECT substr(packfam.PackageFamilyName, instr(packfam.PackageFamilyName, '.') + 1,
    instr(packfam.PackageFamilyName, '_') -2 - instr(packfam.PackageFamilyName, '.') + 1 ) as AppName,
datetime((packuser.installTime/10000000) -11644473600, 'unixepoch') InstallTime,
CASE WHEN instr(pack.PublisherDisplayName, 'ms-resource')=0 THEN pack.PublisherDisplayName
    ELSE '' END AS PublisherDisplayName,
packfam.PublisherId, packuser.User, userkey.UserId,
CASE Architecture
    WHEN 0 THEN 'X64'
    WHEN 9 THEN 'x86'
    WHEN 11 THEN 'Neutral'
    ELSE Architecture END AS Architecture,
substr(pack.packageFullName, instr(pack.packageFullName, '_') + 1,
    instr(substr(pack.packageFullName, instr(pack.packageFullName, '_') + 1), '_') - 1) AS version,
CASE SignatureOrigin
    WHEN 3 THEN 'System'
    WHEN 2 THEN 'Store'
    ELSE 'Unknown' END AS SignatureKind,
packloc.installedLocation
FROM PackageUser packuser, package pack, MrtPackage mrt, packageFamily packfam, packageLocation packloc, User userkey
WHERE packuser.package = pack._PackageId
    AND pack.packageFamily = packfam._PackagefamilyId
    AND packuser.user = userkey._UserID
    AND packloc.package = pack._packageId
    AND (pack.resourceId IS NULL OR pack.resourceId = 'neutral')
)
```

*This is a modified version of the original query written by Mark McKinnon
This works in all versions of Windows 10 including 19H1*

Query Output

AppName	InstallTime	PublisherDisplayName	PublisherId	User	UserSid	Architecture	Version	SignatureKind	inst
WindowsFeedbackHub	2018-09-07 11:27:06	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	1.1805.2331.0	Store	C:\Program File
MicrosoftOfficeHub	2018-09-08 10:43:44	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	17.10314.317...	Store	C:\Program File
WindowsAlarms	2018-09-08 10:44:17	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	10.1804.1101...	Store	C:\Program File
People	2018-09-08 10:45:55	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	10.3.3472.2000	Store	C:\Program File
WindowsSoundRecorder	2018-09-08 10:46:43	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	10.1804.911...	Store	C:\Program File
WindowsCalculator	2018-09-18 23:23:01	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	10.1804.2492.0	Store	C:\Program File
Print3D	2018-09-27 09:11:37	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	3.1.2612.0	Store	C:\Program File
Getstarted	2018-10-09 09:23:19	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	6.15.12641.0	Store	C:\Program File
WindowsMaps	2018-10-13 19:08:50	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	5.1809.2762.0	Store	C:\Program File
Messaging	2018-11-08 20:42:41	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	4.1810.2922.0	Store	C:\Program File
OneConnect	2018-11-17 01:30:51	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	3.1811.3082.0	Store	C:\Program File
XboxIdentityProvider	2018-12-04 15:12:42	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	12.46.25001.0	Store	C:\Program File
Microsoft3DViewer	2018-12-05 12:03:01	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	5.1811.27012.0	Store	C:\Program File
MSPaint	2018-12-05 12:03:27	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	5.1811.20017.0	Store	C:\Program File
MicrosoftSolitaireCollection	2018-12-11 02:18:51	Microsoft Studios	8wekyb3d8bbwe	4	BLOB	X64	4.2.11280.0	Store	C:\Program File
Xbox.TCUI	2018-12-11 02:18:55	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	1.24.10001.0	Store	C:\Program File
BingWeather	2018-12-14 19:25:15	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	4.28.3242.0	Store	C:\Program File
windowscommunicationsapps	2018-12-18 10:43:17	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	16005.11029....	Store	C:\Program File

All installation History

```
2 select User, HResult,
3 (select PackageFullName from PackageIdentity where PackageIdentity._PackageIdentityID=DeploymentHistory.PackageIdentity) as PkgFullName,
4 datetime((WhenOccurred / 10000000) - 11644473600, 'unixepoch') when_occurred
5 from DeploymentHistory
```

	User	HResult	PkgFullName	when_occurred
167	2	0	Microsoft.BingWeather_4.28.10351.0_neutral_~_8wekyb3d8bbwe	2019-02-15 16:57:19
168	2	0	Microsoft.OneConnect_3.1811.3082.0_neutral_~_8wekyb3d8bbwe	2019-02-15 16:57:49
169	2	0	Microsoft.MicrosoftSolitaireCollection_4.2.11280.0_neutral_~_8wekyb3d8bbwe	2019-02-15 16:59:04
170	2	0	9E2F88E3.Twitter_6.1.4.1000_neutral__wgeqdkkx372wm	2019-02-15 16:59:14
171	2	0	Microsoft.SkypeApp_14.39.180.0_neutral_~_kzf8qxf38zg5c	2019-02-15 17:01:57
172	2	0	king.com.CandyCrushSodaSaga_1.132.300.0_x86__kgqvnymyfvs32	2019-02-15 17:02:00
173	2	0	Microsoft.Windows.Photos_2019.18114.17710.0_neutral_~_8wekyb3d8bbwe	2019-02-15 17:02:07
174	2	0	Microsoft.Windows.CloudExperienceHost_10.0.17134.1_neutral_neutral_cw5n1h2txyewy	2019-02-15 18:48:58
175	2	0	Microsoft.AAD.BrokerPlugin_1000.17134.1.0_neutral_neutral_cw5n1h2txyewy	2019-02-15 18:48:58
176	2	0	Microsoft.Windows.ShellExperienceHost_10.0.17134.112_neutral_neutral_cw5n1h2txyewy	2019-02-15 18:49:07
177	2	0	windows.immersivecontrolpanel_10.0.2.1000_neutral_neutral_cw5n1h2txyewy	2019-02-15 18:49:08
178	2	0	Microsoft.Windows.Cortana_1.10.7.17134_neutral_neutral_cw5n1h2txyewy	2019-02-15 18:49:09
179	2	0	Microsoft.Windows.ContentDeliveryManager_10.0.17134.1_neutral_neutral_cw5n1h2txyewy	2019-02-15 18:49:10
180	2	0	Microsoft.MicrosoftEdge_42.17134.1.0_neutral__8wekyb3d8bbwe	2019-02-15 18:49:10
181	2	0	microsoft.windowscommunicationsapps_16005.11029.20108.0_neutral_~_8wekyb3d8bbwe	2019-02-15 18:50:32

Uninstalled
App

App settings from Settings.dat

Viewing settings.dat using regedit's Load Hive option

The hive is located at
%LocalAppData%\Packages\<APP>\Settings

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\settings.dat\LocalState\TVCU

Name	Type	Data
(Default)	REG_SZ	(value not set)
BuddyDisplayName	0x5f5e10c	4b 00 68 00 61 00 74 00 72 00 69 00 2c 00 20 00 59 00 6f 00
BuddyLoginName	0x5f5e10c	6b 00 68 00 61 00 74 00 72 00 69 00 40 00 63 00 68 00 61 00
BuddyLoginTokenAES	0x5f5e114	be 9c b2 af cc 55 f5 54 fe f4 c5 42 30 96 46 b4 ef 18 13 6f 00
BuddyLoginTokenID	0x5f5e104	1c 80 f5 5a 83 c6 f9 36 e2 ce d4 01
BuddyLoginTokenSecretAES	0x5f5e114	21 08 b4 b4 13 e2 58 f4 8d e7 71 91 f5 f8 8c e8 25 37 94 f0 00
LastDisplayedGroup	0x5f5e104	26 12 88 04 af 04 96 1a 76 c5 d4 01
MetroLastSelectedTab	0x5f5e104	01 00 00 00 87 c3 50 86 e2 ce d4 01

Edit Binary Value

Value name: BuddyDisplayName

Value data:

0000	4B 00 68 00 61 00 74 00	K.h.a.t.
0008	72 00 69 00 2C 00 20 00	r.i.. .
0010	59 00 6F 00 67 00 65 00	Y.o.g.e.
0018	73 00 68 00 00 00 0F A7	s.h....\$
0020	8C 1A 76 C5 D4 01	..vÅ.

OK Cancel

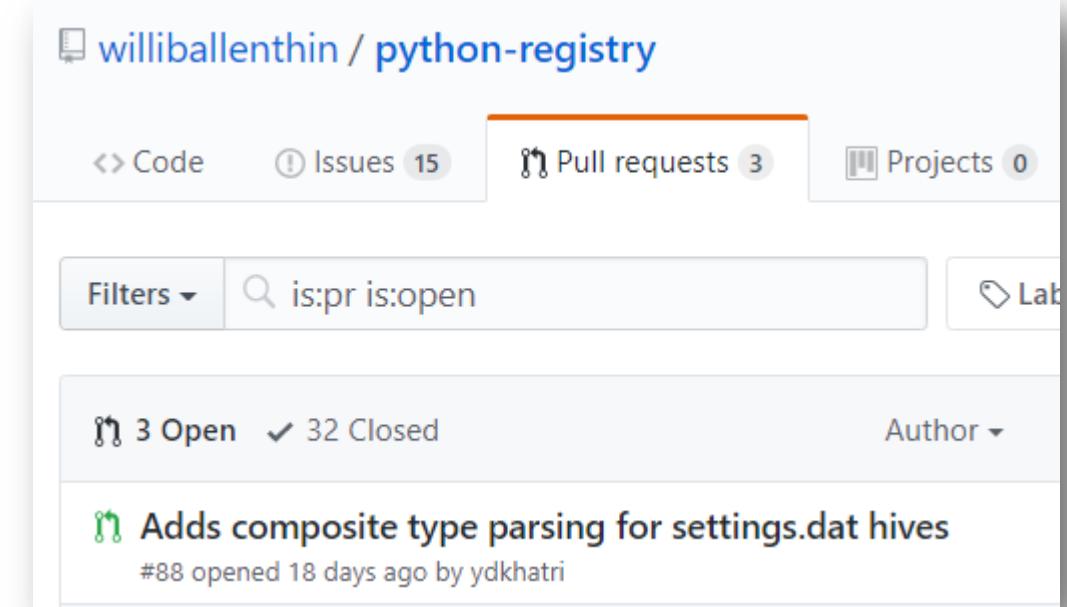
Every Value has a Last Modified timestamp

Settings.dat – New data types

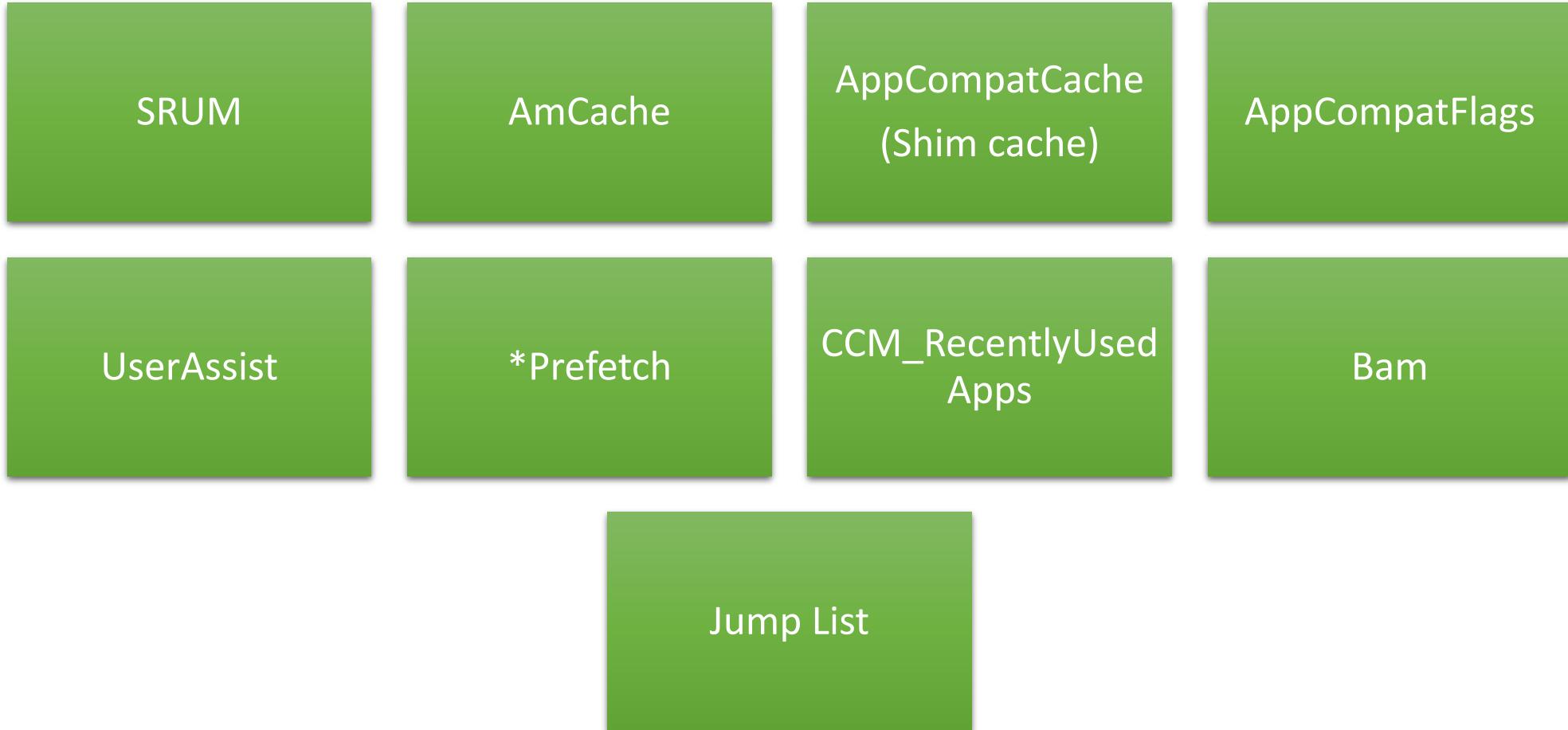
Reg Type Last byte (hex)	Data type
01	uint8
02	int16
03	uint16
04	int32
05	uint32
06	int64
07	uint64
08	Float / Single
09	Double
0A	Unicode char
0B	Boolean
0C	Unicode String
0D	Application Data Composite Value (Dictionary Object)
0E	DateTimeOffset (timestamp)
0F	TimeSpan (100ns ticks)

Reg Type Last byte (hex)	Data Type
10	GUID
11	?
12	?
13	?
14	bytes array
15	int16 array
16	uint16 array
17	int32 array
18	uint32 array
19	int64 array
1A	uint64 array
1B	Float array
1C	Double array
1D	Unicode char array
1E	Boolean array
1F	Unicode string array

All discovered types added to **python-registry**



App execution trace artifacts



** Some apps like Twitter do not have an exe*

App execution traces – Jumplist CustomDest

The screenshot shows the interface of JumpList Explorer v0.8.1.0. On the left, there's a tree view of custom destinations under 'Source File Name' and a list of items under 'Name'. A specific item is selected: 'Lnk #: 000 - 41747ArnoKlenke.AEScryptor_1wb57y56r5xww!App'. The main pane displays detailed information about this link, including its source file path (C:\ZimmermanTools\Offset_0x18.lnk), target ID (41747ArnoKlenke.AEScryptor_1wb57y56r5xww!App), type (File), and extension blocks. A green box highlights the 'Extra blocks information' section, which lists various properties and their values, such as AppUserModel ID (41747ArnoKlenke.AEScryptor_1wb57y56r5xww!App) and Title (Spreadsheet.copy.xlsx). The status bar at the bottom shows the full path of the selected item.

JumpList Explorer v0.8.1.0

File Tools Help

Drag a column header here to group by that column

Source File Name

RBC

C:\Users\khatri\Desktop\TEMP_TEST\CustomDestinations\1c7a9b
C:\Users\khatri\Desktop\TEMP_TEST\CustomDestinations\1ced32
C:\Users\khatri\Desktop\TEMP_TEST\CustomDestinations\7f061f
C:\Users\khatri\Desktop\TEMP_TEST\CustomDestinations\9d1f90
C:\Users\khatri\Desktop\TEMP_TEST\CustomDestinations\590aaee

Name

7f061f3d82b342d0.customDestinations-ms

Lnk #: 000 - 41747ArnoKlenke.AEScryptor_1wb57y56r5xww!App

Lnk #: 001 - 41747ArnoKlenke.AEScryptor_1wb57y56r5xww!App

Properties

Loaded Lnk ==> 41747ArnoKlenke.AEScryptor_1wb57y56r5xww!App

Lnk details: Offset_0x18.lnk

Details Details as string

Source file: C:\ZimmermanTools\Offset_0x18.lnk

Source created:

Source modified:

Source accessed:

--- Target ID information ---

>>Short name: 41747ArnoKlenke.AEScryptor_1wb57y56r5xww!App

Type: File, Value: 41747ArnoKlenke.AEScryptor_1wb57y56r5xww!App

Extension blocks found: 1

----- Block 0 (Beef0004) -----

Long name: 41747ArnoKlenke.AEScryptor_1wb57y56r5xww!App

Created:

Last access:

--- Extra blocks information ---

>>Property store data block (Format: GUID)\ID Description ==> Value)		
9f4c2855-9f79-4b39-a8d0-e1d42de1d5f3\28	(Description not available)	==>
9f4c2855-9f79-4b39-a8d0-e1d42de1d5f3\27	(Description not available)	==> Spreadsheet.copy.xlsx
9f4c2855-9f79-4b39-a8d0-e1d42de1d5f3\30	(Description not available)	==>
9f4c2855-9f79-4b39-a8d0-e1d42de1d5f3\5	AppUserModel ID	==> 41747ArnoKlenke.AEScryptor_1wb57y56r5xww!App
9f4c2855-9f79-4b39-a8d0-e1d42de1d5f3\20	(Description not available)	==> 0bda02c92faa2c27a13b8be7393ceac3
f29f85e0-4ff9-1068-ab91-08002b27b3d9\2	Title	==> Spreadsheet.copy.xlsx
436f2667-14e2-4feb-b30a-146c53b5b674\100	(Description not available)	==> 0bda02c92faa2c27a13b8be7393ceac3

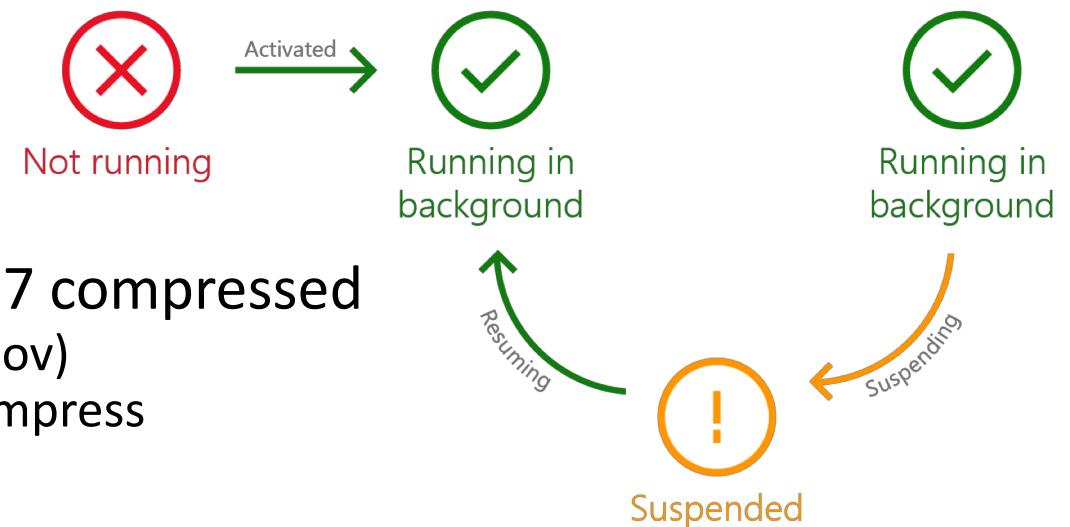
C:\Users\khatri\Desktop\TEMP_TEST\CustomDestinations\7f061f3d82b342d0.customDestinations-ms

swapfile.sys

- Per Microsoft:

“A UWP app is suspended shortly after the user minimizes it or switches to another app. This means that the app's threads are stopped and the app is left in memory unless the operating system needs to reclaim resources. When the user switches back to the app, it can be quickly restored to a running state.”

- Suspended app memory pages are moved to **C:\swapfile.sys**



- In windows 10, pages swapped may be LZ77 compressed
 - Use `winmem_decompress` (from Maxim Suhanov)
 - https://github.com/msuhanov/winmem_decompress

UsrClass.dat

- PersistedStorageItemTable reg key in
 - HKEY_CURRENT_USER\Software\Classes = Usrclass.dat
 - \Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\<App Pkg FamilyName>\PersistedStorageItemTable\ManagedByApp

The screenshot shows the Windows Registry Editor window. The title bar reads "Registry Editor". The menu bar includes "File", "Edit", "View", "Favorites", and "Help". The toolbar has standard icons for file operations. The status bar at the bottom shows the path "Computer\HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Photos_8wekyb3d8bbwe\PersistedStorageItemTable\ManagedByApp".

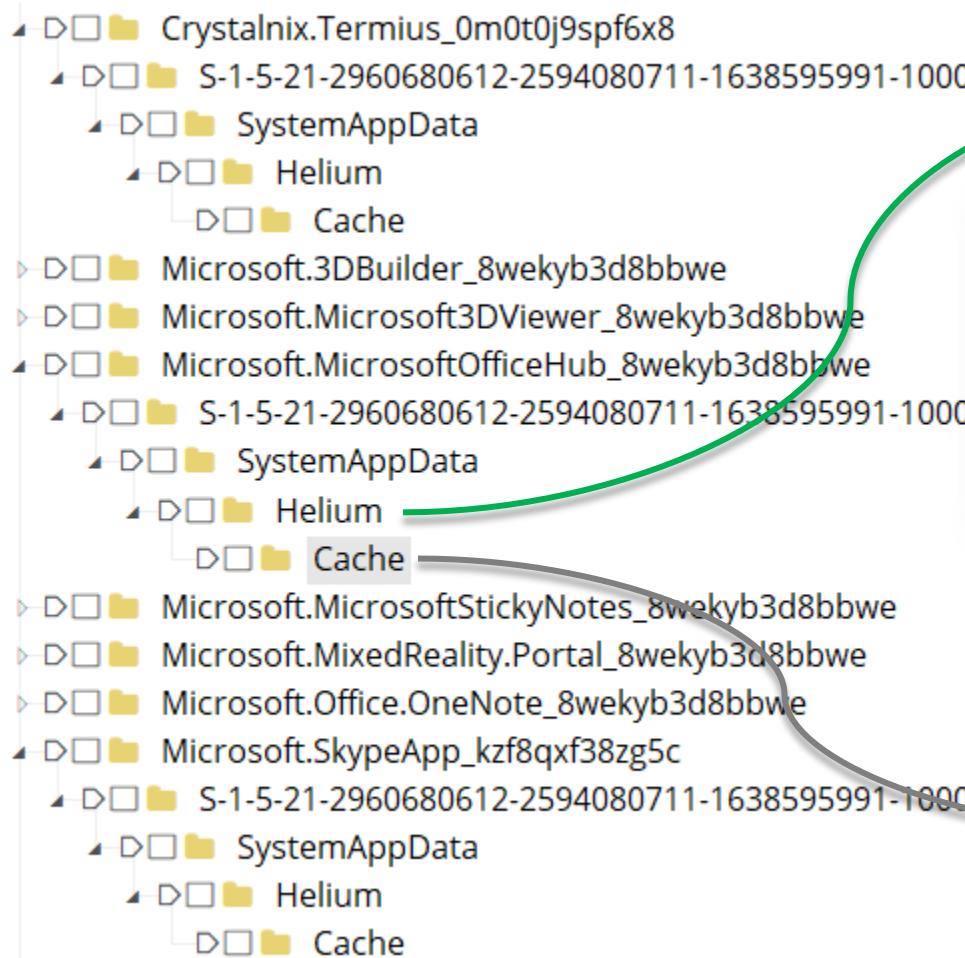
The left pane displays a tree view of registry keys under "Microsoft.Windows.Photos_8wekyb3d8bbwe". The "PersistedStorageItemTable" key is expanded, showing its subkeys: "ManagedByApp", "{1F6F6472-E3C1-49D4-B1DF-B85740331C0A}", "{5E8D9144-C39B-493D-BEEA-55721C69B4F5}", and "{62439C51-1C19-49E3-A367-25A567F169DA}". The "ManagedByApp" key is selected.

The right pane shows a table of registry values for the "ManagedByApp" key:

Name	Type	Data
(Default)	REG_SZ	(value not set)
FilePath	REG_SZ	\?\Volume(70F93006-0000-0000-0000-F01500000000)\Dropbox\AppBar_research\jumplist\aesEncryptor.customdest1.PNG
Flags	REG_DWORD	0x00000009 (9)
LastUpdatedTime	REG_BINARY	c4 6d 47 07 4b e4 d4 01
Link	REG_BINARY	01 14 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 4c 00 00 00 01 14 02 00 00 00 00 c0 00 00 00 00 00 46 83 00 00 00
Metadata	REG_SZ	0 G:\Dropbox\AppBar_research\jumplist\aesEncryptor.customdest1.PNG
PackageFamilyName	REG_SZ	Microsoft.Windows.Photos_8wekyb3d8bbwe
SystemVisible	REG_DWORD	0x00000000 (0)

Several values in the table are highlighted with red boxes: "FilePath", "LastUpdatedTime", and "Metadata".

More registry hives @ C:\ProgramData\Packages\<APP Family Name>



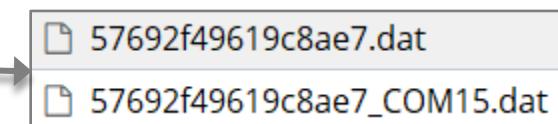
A screenshot of a user activity log table. The columns are: Program Name, Run Counter, Focus Count, Focus Time, and Last Executed. The data shows:

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
RBC	=	=	RBC	=
Microsoft.Office.OneNote_8wekyb3d8bbwe!microsoft.onenoteim	1	2	0d, 0h, 02m, 04s	2019-03-07 14:23:15
UEME_CTLSESSION	237	912	0d, 11h, 30m, 40s	
Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge	7	43	0d, 0h, 09m, 56s	2019-03-07 14:28:18

User info & artifacts here

User.dat →

Software\Microsoft\Windows\CurrentVersion\Explorer\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count



Mostly empty, no user artifacts

Remnants after uninstall

The screenshot shows the Windows Registry Editor window. The title bar reads "Registry Editor". The menu bar includes "File", "Edit", "View", "Favorites", and "Help". The address bar displays the path "Computer\HKEY_CURRENT_USER\Software\Microsoft\UserData\UninstallTimes".

The left pane shows a tree view of registry keys under "UserData": ChatRT, UninstallTimes (selected), WAB, WcmSvc, and wfs.

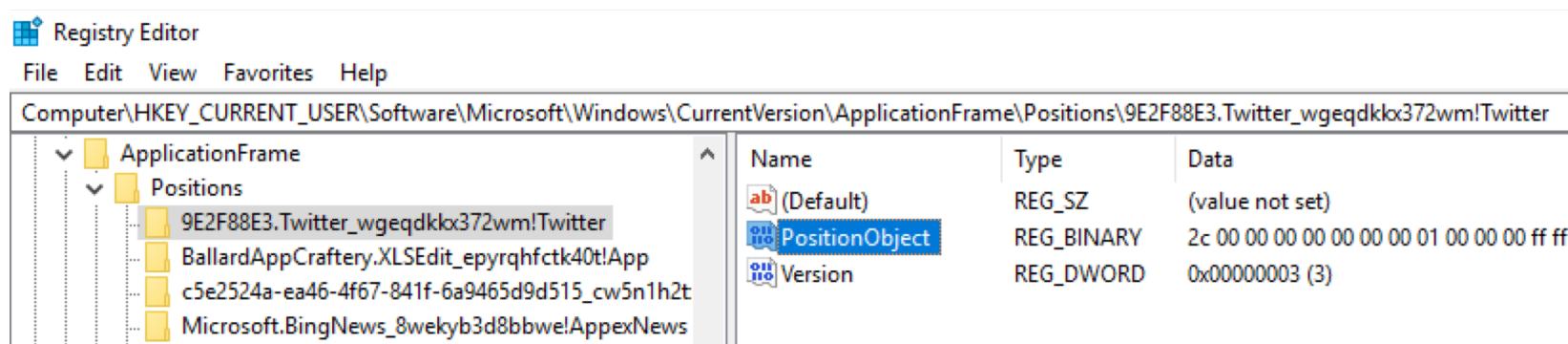
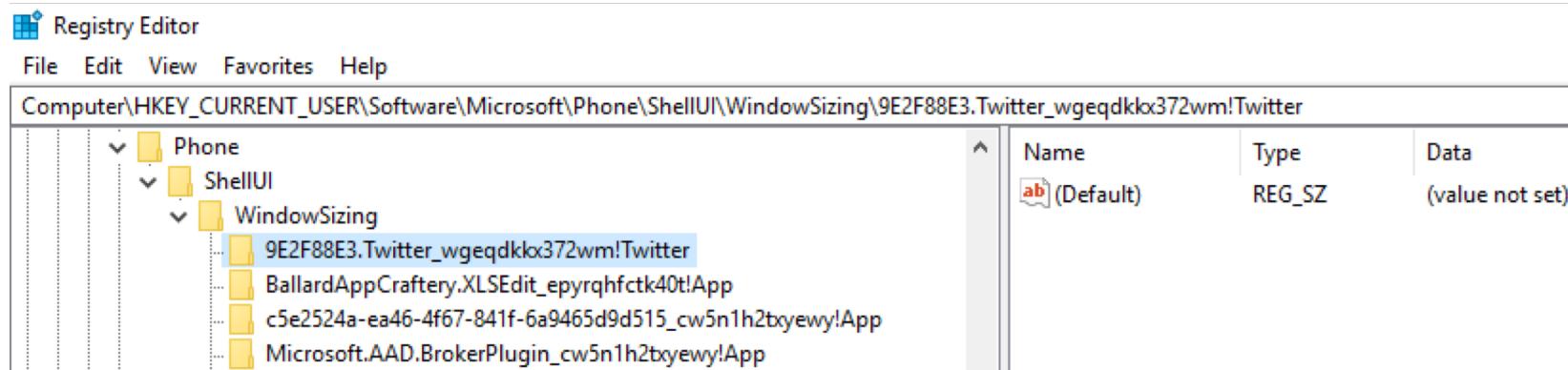
The right pane displays a table of registry values:

Name	Type	Data
(Default)	REG_SZ	(value not set)
9E2F88E3.Twitter_wgeqdkkx372wm	REG_BINARY	19 1f 07 0d 46 d4 d4 01
Microsoft.Windows.SecondaryTileExp...	REG_BINARY	c5 4a 26 1f 5f c5 d4 01
Microsoft.WindowsFeedback_cw5n1h...	REG_BINARY	a2 d3 84 0f b9 2b d2 01

A red circle highlights the value name "9E2F88E3.Twitter_wgeqdkkx372wm" and its data value "19 1f 07 0d 46 d4 d4 01". A red arrow points from this highlighted area to a timestamp at the bottom right.

At the bottom right, a red rounded rectangle contains the text "Wed, 06 March 2019 17:57:23 UTC".

Leftovers..



We found at least another 10 locations in the registry where you can find remnants of old Uninstalled Apps

These locations have to do with MrtCache, Push Notification settings, more window positioning and cached Capability settings

Webcache – IE/Edge database

- WebcacheV01.dat
 - C:\Users\<USER>\AppData\Local\Microsoft\Windows\WebCache\

The screenshot shows the ESEDatabaseView application interface. The title bar reads "ESEDatabaseView: C:\Users\khatri\Desktop\AppxCode\WebCache\WebCacheV01.dat". The menu bar includes File, Edit, View, Options, and Help. Below the menu is a toolbar with icons for file operations. The main window has two panes. The left pane displays a list of tables under the heading "AppCacheEntryEx_1 [Table ID = 15, 15 Columns]". A green box highlights the first 25 entries of this list. The right pane displays a list of URLs under the heading "Url", also with a green box highlighting the first few entries.

Table ID	Column Count
BlobEntry_79	8
BlobEntry_84	8
BlobEntry_87	8
Container_1	25
Container_10	25
Container_100	25
Container_101	25
Container_11	25
Container_12	25
Container_13	25
Container_14	25
Container_15	25
Container_16	25
Container_17	25
Container_18	25
Container_19	25
Container_2	25
Container_20	25
Container_21	25
Container_22	25
Container_23	25
Container_24	17
Container_25	25
Container_26	25

URL
https://www.bing.com/rb/G/cir2,ortl,cc,nc/4dceb7eb/1448f34b.css?bu=COwH-QaDCLQGtAb7B_cHtAY
https://www.bing.com/rb/G/cj,nj/56eb060c/05e167be.js?bu=F40E0gLUAtgC1gLDAr8CpAL8AfkBnQLFAscCygKaAocCtgWu
https://www.bing.com/rb/G/cj,nj/5dad9aec/57ff1e62.js?bu=HcEEwwTXBNUE8QTvBOEE4wTdBNNEzwTTBM0EywTzBPgEyQ
https://www.bing.com/rb/G/cj,nj/6629ae9f/f6d5d5e2.js?bu=G7QBiQKuAoMCjwKSArACuQKyArQCtwG5Ae4B8AGYAvMBnv
https://www.bing.com/rms/BingCore.Bundle/cj,nj/3a2ff3e0/5be92d0f.js?bu=rms+answers+Shared+BingCore%24ClientIn:
https://www.bing.com/rs/2u/2J/ortl,cc,nc/035dcc18/3fe43eeb.css
https://www.bing.com/rs/2w/6/cj,nj/abd90c55/8cafcc5f.js
https://www.bing.com/rs/5X/H/cj,nj/7e516373/53c747e0.js
https://www.bing.com/rs/5k/G/nj/8fe7be63/8636b4dd.js
https://www.bing.com/rs/5k/p/nj/d9799f53/045d3532.js
https://www.bing.com/rs/6o/xF/ortl,cc,nc/d3857dc2/2743db28.css
https://www.bing.com/rs/G/3o/cj,nj/c5ee6d4b/359d2aee.js

PartitionsEx Table

TableId	Partition Type	PartitionId	Directory	
9	0	M	C:\Users\ROXY\AppData\Local\Microsoft\Windows\AppCache\RBY7JR OD	<i>L=Low integrity, M=Medium</i>
10	1	M	C:\Users\ROXY\AppData\Local\Microsoft\Windows\INetCache\IE	
19	4	M	C:\Users\ROXY\AppData\Local\Microsoft\Windows\INetCache\IE	
20	3	M	C:\Users\ROXY\AppData\Local\Microsoft\Windows\INetCookies\ESE\	
34	2	M	C:\Users\ROXY\AppData\Local\Microsoft\Windows\INetCache\IE	
18	3	S-1-15-2-1063257880-1914585122- 1954150059-946145533-116938067- 416079064-1690466945	C:\Users\ROXY\AppData\Local\Packages\9e2f88e3.twitter_wgeqdkkx3 72wm\AC\INetCookies\ESE\	
32	4	S-1-15-2-1609473798-1231923017- 684268153-4268514328-882773646- 2760585773-1760938157	C:\Users\ROXY\AppData\Local\Packages\microsoft.windowsstore_8we kyb3d8bbwe\AC\INetCache	
33	3	S-1-15-2-1609473798-1231923017- 684268153-4268514328-882773646- 2760585773-1760938157	C:\Users\ROXY\AppData\Local\Packages\microsoft.windowsstore_8we kyb3d8bbwe\AC\INetCookies\ESE\	

Table Names & Mapping

PartitionType value	Table holding data	Table content type
0	AppCacheEntryEx_*	Cached URL & file info
0	AppCacheEx_*	Cached URL & file info
1	DependencyEntryEx_*	Domains referenced by content in given URL
2	HstsEntryEx_*	Domain info?
3	CookieEntryEx_*	Cookie data
4	BlobEntry_*	Certificate blobs

18	3	S-1-15-2-1063257880-1914585122-1954150059-946145533-116938067-416079064-1690466945	C:\Users\ROXY\AppData\Local\Packages\9e2f88e3.twitter_wgeq72wm\AC\INetCookies\ESE\
----	---	--	--

CookieEntryEx_18 ← Resulting table name

Containers Table

- Provides data types & mapping for *Container_** tables

ContainerId	Name	PartitionId
1	Content	M
2	History	M
3	Cookies	S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-2659745135-2630312742
4	Content	S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-2659745135-2630312742
5	DOMStore	S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-2659745135-2630312742
6	Content	S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194
7	MicrosoftEdge_iecompat	M
8	MicrosoftEdge_iecompatua	M
9	Content	S-1-15-2-350187224-1905355452-1037786396-3028148496-2624191407-3283318427-1255436723
10	Cookies	S-1-15-2-350187224-1905355452-1037786396-3028148496-2624191407-3283318427-1255436723
11	BackgroundTransferApi	S-1-15-2-350187224-1905355452-1037786396-3028148496-2624191407-3283318427-1255436723

Querying All_Container view

```
SELECT App, Type, datetime((AccessedTime/10000000) -11644473600, 'unixepoch') AccessedTime, AccessCount, URL  
FROM ALL_Container
```

App	Type	AccessedTime	AccessCount	Url
bingnews	DOMStore	2019-02-19 21:43:13	1	DOMStore: https://connexity.net/
bingnews	DOMStore	2019-02-19 22:12:03	1	DOMStore: https://www.incredibleindia.org/
bingnews	DOMStore	2019-02-19 21:22:45	1	DOMStore: https://ads.pubmatic.com/
xlsedit	Content	2019-03-14 20:56:06	3	http://ajax.googleapis.com/ajax/libs/jquery/2.1.3/jquery.min.js
xlsedit	Content	2019-03-14 20:56:06	3	http://d1t2zu1r5z6kzt.cloudfront.net/cookies.js
xlsedit	Content	2019-03-14 20:52:29	1	http://cdn.softserver.co/v2/?flow=120&lang=en-US&uwp=true&slot=sheetedit
xlsedit	Content	2019-03-14 20:56:03	2	http://cdn.softserver.co/v2/?flow=121&lang=en-US&uwp=true&slot=sheetedit
xlsedit	Content	2019-03-14 20:56:06	1	http://static.fassets.net/creative/recycle-bin.png
xlsedit	Content	2019-03-14 20:55:31	2	http://static.fassets.net/creative/pdf/download-reader.gif
xlsedit	Content	2019-03-14 20:53:31	2	http://static.fassets.net/creative/download-notification.gif
xlsedit	Content	2019-03-14 20:52:31	2	http://static.fassets.net/creative/usb-icon.png
xlsedit	Content	2019-03-14 20:56:30	1	http://static.fassets.net/creative/winopener.gif
xlsedit	DOMStore	2019-03-14 20:52:29	1	DOMStore: http://cdn.softserver.co/
MicrosoftOfficeHub	History	2019-03-07 14:18:56	3	Visited: ROXY@ https://contentstorage.osi.office.net/getofficecarouselcore/index
MicrosoftOfficeHub	History	2019-03-07 14:18:22	2	Visited: ROXY@ https://odc.officeapps.live.com/odc/v2.0/hrd?lcid=1033&syslcid

New Shiny Tools...

DEMO

Thanks for listening!

Any Questions?



Tools @ <https://github.com/ydkhatri/Appx-Analysis>



@*swiftforensics*
@*jackfarley248*



Yogesh@*swiftforensics.com*
Jack.Farley@mymail.champlain.edu

References to tools and resources

- Windows Internals Seventh Edition Part 1 - Pavel Yosifovich; David A. Solomon; Mark E. Russinovich; Alex Ionescu
- TokenView - <https://github.com/googleprojectzero/sandbox-attacksurface-analysis-tools>
- [The Inner Workings of the Windows Runtime.pdf](#) – James Forshaw
- Store and retrieve settings and other app data - <https://docs.microsoft.com/en-us/windows/uwp/design/app-settings/store-and-retrieve-app-data>
- ApplicationDataCompositeValueClass - <https://docs.microsoft.com/en-us/uwp/api/windows.storage.applicationdatacompositevalue>
- python-registry - <https://github.com/williballenthin/python-registry>
- Parses APPX programs - https://medium.com/@markmckinnon_80619/parse-the-appx-programs-in-autopsy-763d9017c4c
- All installed apps - <https://boncaldoforensics.wordpress.com/2018/10/07/all-installed-apps-artifact-windows-10-forensics/>
- App Lifecycle - <https://docs.microsoft.com/en-us/windows/uwp/launch-resume/app-lifecycle>